

MOBILITY SUPPORT USING INTELLIGENT USER SHADOWS FOR NEXT-GENERATION WIRELESS NETWORKS

Gergely V. Záruba, Wei Wu, Mohan J. Kumar, Sajal K. Das
Center for Research in Wireless Mobility and Networking
Department of Computer Science and Engineering
The University of Texas at Arlington
Arlington, Texas, USA 76019
{zaruba, wuwei, kumar, das}@cse.uta.edu

Abstract

This paper proposes a mobility management scheme for seamless roaming in fourth generation (4G) wireless overlay networks. A new mobile software entity called user shadow is introduced to the wired network, addressing the roaming needs of the mobile user. With the help of these user shadows, most signaling interaction between mobile devices and wired networks is constrained to the wired links, reducing the dependence on the limited wireless bandwidth. Additionally, the novel concept of software IP mobility is introduced, enabling the mobile software entities (i.e., user shadows) to communicate using their own IP stack. Software IP mobility enhances the current IP mobility approaches while helping in providing with seamless mobility. A signaling cost analysis is performed to compare signaling overhead of the user shadow approach to that of Mobile IP.

1. Introduction

One of the major enablers towards next generation (NG or 4G) wireless networks is *system integration* [1,2] where a unique perception general wireless access system is to be established through the integration of the services offered by current (such as UMTS, GPRS, Wireless LAN, etc.) and future wireless access technologies. The trend towards packet switched technologies and increasingly general use/acceptance of the Internet Protocol (IP) indicate that all these wireless access networks are to be connected to an IP-based core network (i.e., the Internet). In other words, NG wireless networks can be seen as many overlapping wireless Internet access domains. In this

heterogeneous environment, a mobile host (MH¹) is equipped with multiple wireless interfaces or a multi-mode wireless interface to connect to any or all wireless access networks *anytime anywhere*. The seamless roaming of a MH in NG wireless networks involves various tasks such as wireless interface management, handoff decision, service admission request and quality of service (QoS) negotiation while considering limited processing power and battery life of the MHs.

In this paper, we describe a mobility management scheme relaying on our 4G system integration framework called NGIneUS (Intelligent User Shadows for Next Generation Wireless Services – pronounced: ingenious) [3]. The motivation behind our work is given by the fact that the processing power and bandwidth of wired networks are relatively easily expandable and thus their extensive use can be justified to most efficiently control the scarcest resource: the wireless bandwidth. One of the novel ideas of our scheme is the deployment of mobile software entities, namely *user shadows* into the wired networks, controlling and negotiating with the network on behalf of the users. User shadows can help to limit the signaling overhead to the wired networks as much as possible. Another new concept in NGIneUS is the assignment of IP addresses to the user shadows, i.e., to mobile *software* entities. Therefore, user shadows can receive and terminate data streams of services to and from corresponding nodes, while individual users need to communicate only with their respective shadows. As users roam, the associated user shadows migrate inside the wired networks, much like shadows, hence the name. Since shadows are assigned their own IP addresses, their

¹ We will use mobile host and mobile user interchangeably in this paper.

migration can be handled by any of the existing IP mobility management protocols (with slight extensions).

Mobile IP [4] is one of the premier IP mobility management protocols standardized by the IETF (Internet Engineering Task Force). Mobile IP relies on the association of a unique IP address with the MH's wireless interface. Mobile IP enables correspondent hosts (CH) to reach the MH through its unique IP address even if the MH resides in a foreign network. A home agent (HA), foreign agents (FA), and temporary IP addresses (care-of addresses) are used to aid packet forwarding. If a MH changes its wireless point of attachment (by roaming between networks), it has to update its location with its HA. The more frequent the handoff requests are the more wireless bandwidth is used for signaling. To reduce the signaling cost for MHs moving within the local domain, intra-domain or micro-mobility management protocols have been proposed, such as Cellular IP [5], HAWAII [6] and IDMP [7]. With such hierarchical schemes, MH mobility generates location update signaling up-to the gateway node only, thus shielding the HA from mobility effects. However, even with these schemes, roaming MHs will still need to transmit location update messages via the wireless links.

In contrast, our scheme requires the user shadows within the wired infrastructure to send location updates on behalf of MHs. Moreover, none of the existing mobility schemes provide any support to the MHs for dealing with mobility-related tasks, whereas user shadows communicate with the network on behalf of the MHs, enhancing network proactivity and user transparency.

The rest of the paper is organized as follows: Section 2 presents the proposed mobility management scheme, reviewing the concepts of user shadows and software IP mobility. Section 3 outlines the comparative signaling cost analysis on our mobility management scheme and Mobile IP. Section 4 concludes the paper.

2. Mobility Support Using User Shadows

NGIneUS considers NG wireless systems to be heterogeneous networks consisting of several overlaying wireless access networks, while MHs are equipped with multiple wireless interfaces. User

shadows are running and migrating between dedicated environments, namely *NG servers (NGS)*. NGSs are deployed in each wireless access domain, co-located with network controllers or routers. For example, in a GSM cellular network, an NGS could be mapped to each mobile service switching center (MSC) controlling several base station controllers (BSC), while in a corporate wireless LAN environment, the NGS could be the gateway router connecting the access points to the rest of the network. An architectural view of NG wireless system is provided in Figure 1.

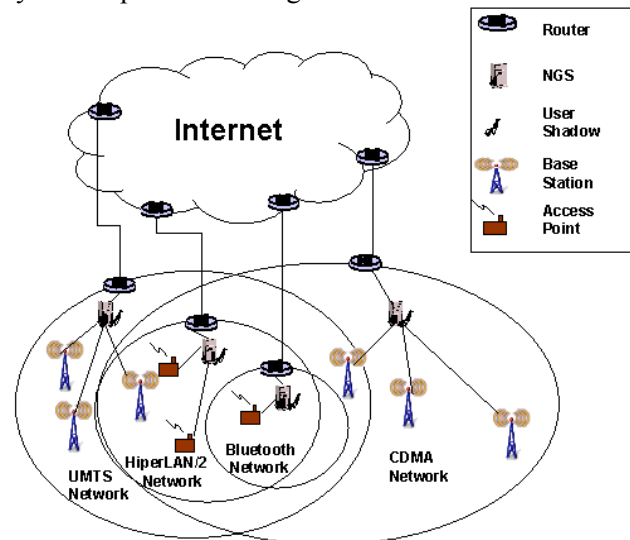


Figure 1. Architecture of NGIneUS using user shadows

2.1. User Shadows

In the proposed mobility management scheme, each mobile user is associated with a user shadow, following the user's path in the wired infrastructure and controlling network access parameters on behalf of the user. As the user moves, the associated shadow will also migrate from one NGS to another in the wired network, optimizing the distance between itself and its owner. It is the task of the user shadows to determine whether to migrate to another NGS based on the current location of users as well as on user profiles, such as mobility patterns, QoS requirements of applications, user subscription plans and capability of the mobile device [3]. The location change of MHs can be detected by intercepting messages of the new IP address assignment to the MH since NGSs are normally co-located with the edge router or gateway,

where IP address assignment functions such as DHCP (Dynamic Host Configuration Protocol) server are configured. The NGS at the access domain to which the MH enters will send a migration notice message to the NGS at the previous access domain of the MH. If multiple wireless air interfaces are available to the MH, the shadow will instruct the MH to use the appropriate wireless interface for communication. In this case, the user shadow (or a copy of the shadow) can migrate in advance to the corresponding NGS. Figure 2 shows the message flow of migration procedure of a user shadow, where the DHCP server in charge of providing with care-of addresses is assumed to be co-located with the NGS in each subnet.

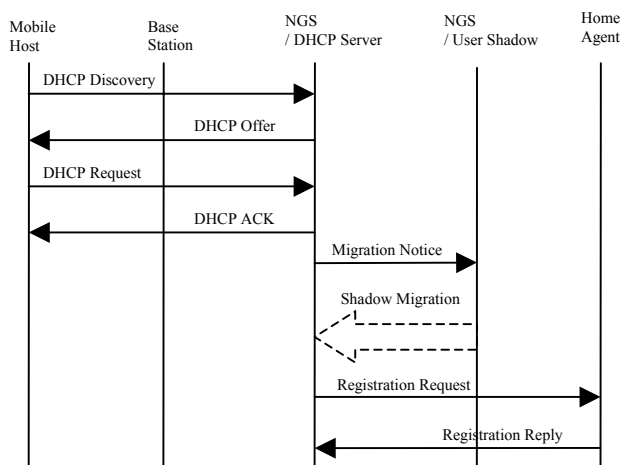


Figure 2. Message flow of shadow migration

Migration is not the only way for user shadows to move closer to the users. The fact, that there is a one-to-one mapping between users and shadows implies that a shadow can only be present at the NGS of one of the wireless interfaces. Yet, the user has to be enabled to use the other available access networks as well. Thus, user shadows can instruct the NGSs of those access networks to spawn a process, which we refer to as the *slave user shadow*. The slave user shadow’s task is to receive/transmit packets to/from the user through the wireless interface relaying those packets to the shadow. Another task of the slave is to negotiate access parameters with the access network controller on behalf of the user (and the shadow). Since slave shadows are access network specific, no data or code migration is initiated by the user

shadow; it simply instructs the NGS to create a new process. User shadows and their slaves communicate through a common protocol, called *inter-shadow messaging protocol* (ISMP).

Another major difference between user shadows and their slaves is that the former have their own IP address while the slaves use the IP address of the corresponding NGS and a port number. While user shadows never cease to exist though they migrate from one NGS to another, slave shadows can as easily be terminated by their masters as they were created; slave user shadows do not carry any important information about the user, her behavior or the properties of her connections. Using this approach one software entity, i.e., the master user shadow can control the information flow arriving and departing simultaneously through various wireless interfaces. Although the message exchange between shadow master and slaves introduces signaling overhead, such messages are within the wired networks, thereby not affecting the bandwidth constrained wireless links. The information collected from the slave shadow plays an important role in the mobility management, stream admission control, scheduling, and profile management.

Figure 3 depicts the slave user shadow spawning procedure where the user is originally connected to only a macro-cell provider thus 100% of her traffic is routed on the only available interface. When the user moves into a hot-spot area, a slave shadow is spawn in the NGS of the hot-spot; 40% of her traffic in the example is routed over the hot-spot’s interface.

2.2. Software IP Mobility

Current IP mobility management proposals deal only with mobility of hardware devices. IP addresses are associated to the wireless interfaces of mobile devices. In NGIneUS, mobile software entities, i.e., user shadows are allowed to be associated with IP addresses, such that applications can address and communicate with mobile software code using a simple IP address. In our proposed scheme, user shadows function as terminating points for IP packets and overlying transport layer (i.e., TCP, UDP) data streams, i.e., it is the user shadows that carry the user specific IP address and terminate all network and transport layer streams. Since user

shadows reside inside NGSs, routing functions have to be included in all NGSs. Routing is to be performed between the IP layer associated with the physical interface of the NGS and the IP stacks of each of the software (virtual) interfaces created by individual user shadows. Figure 4 outlines the protocol stack in NGS.

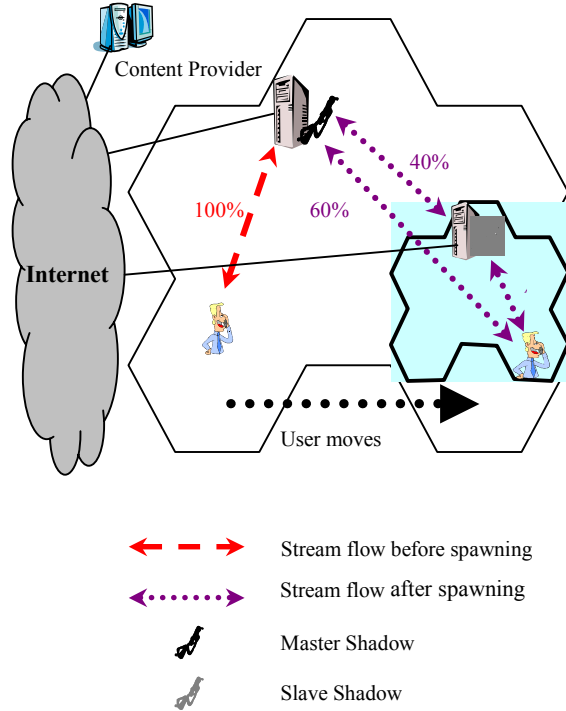


Figure 3. Master vs. slave user shadows

User shadows create their own virtual (software) interface; thus each user shadow has its own TCP/IP protocol stack and routes all the packets to the default IP of the NGS IP layer. Similar to the IP address assignment to a physical mobile device using Mobile IP, a user shadow can also have its home IP address and care-of-address in the foreign networks. Alternatively, the shadow IP address can be acquired from any DHCP server with dynamic update to the DNS server. In other words, user shadows can be treated just like “mobile devices” and as such devices, they need IP mobility handling; since user shadows are software agents, we refer to their mobility as software IP mobility.

With the unique IP address associated to shadows, they can always be reached even after migrating to a new NGSs. Since a mobile user is represented by its shadow to the outside world, a

binding mechanism is needed between the user and her shadow. To update the binding with the shadow, the mobile user sends refreshing messages to the NGS in the same domain periodically or on-demand. In turn, the NGS relays the message to the corresponding user shadow by checking the MAC address of the mobile device.

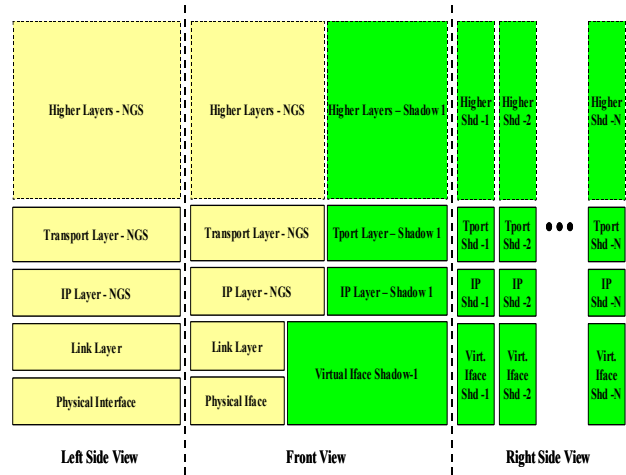


Figure 4. NGS protocol stack

3. Signaling Cost Analysis

In this section, we perform a simple signaling cost analysis in terms of location update cost on NGIneUS, while comparing the results to the signaling cost of Mobile IP. We select Mobile IP as the manager to handle the mobility of user shadows, and assume that MH care-of addresses are assigned by a DHCP server. For simplicity, user shadow spawning is not considered. To create a simple, comparable situation with Mobile IP, a MH is assumed to use co-located care-of-address in the foreign network (configured using the DHCP server). The DHCP server is assumed to be co-located with the NGS in each subnet. The mobility pattern of users is modeled by the fluid flow model [8], where MHs are uniformly distributed with a density ρ and move at an average velocity of v in uniformly distributed directions (between $[0, 2\pi)$). If the subnet areas are square-shaped with the perimeter l , the subnet-crossing or handoff rate of a MH is $r_c = \rho * v * l / \pi$.

We define the following parameters for the signaling cost analysis: C_{mh-bs} is the transmission cost between MHs and base stations. $C_{bs-dhcp}$ is the transmission cost between the base station and the

NGS/DHCP server of the subnet, which the MH moves to. $C_{dhcp-dhcp}$ is the transmission cost between the NGS/DHCP server in the MH's current subnet and the NGS/DHCP server in the MH's previous subnet. $C_{dhcp-ha}$ is the transmission cost between the NGS/DHCP server in the MH's current subnet and the home agent. Based on the message flow shown in Figure 2, the signaling cost of the user shadow scheme can be expressed as:

$$C_{shadow} = 4C_{mh-bs} + 4C_{bs-dhcp} + 2C_{dhcp-dhcp} + 2C_{dhcp-ha} \quad (1)$$

The DHCP address acquiring procedure is same for the MH using Mobile IP. The difference is that the MH itself has to send the registration request to the HA, and HA replies directly to the MH. So, wireless transmission is required for the location update of the MH. Thus, the signaling cost of Mobile IP can be expressed as:

$$C_{mip} = 6C_{mh-bs} + 6C_{bs-dhcp} + 2C_{dhcp-ha} \quad (2)$$

Let $H_{bs-dhcp}$ be the average number of hops between base station and NGS/DHCP server, $H_{dhcp-dhcp}$ be the average number of hops between any two NGSs/DHCP servers, and $H_{dhcp-ha}$ be the average number of hops between NGS/DHCP server and HA. The transmission cost is assumed to be proportional to the distance between the two end-points, the proportionality constant being δ . We assume the transmission cost over wireless links to be α times higher than that over wired links; since the transmission cost over the wireless links is much higher than that over wired links $\alpha \gg 1$. Shadow migration requires the transmission of the software code from one NGS to another generating β times higher cost than normal signaling message transmission. Using the above methodology, the signaling cost per time unit with NGIneUS can be expressed as:

$$\begin{aligned} C_{shadow} &= (4\alpha H_{mh-bs} + 4H_{bs-dhcp} + (\beta+1)H_{dhcp-dhcp} + 2H_{dhcp-ha})\delta r_c \\ &= (4\alpha H_{mh-bs} + 4H_{bs-dhcp} + (\beta+1)H_{dhcp-dhcp} + 2H_{dhcp-ha})\frac{\rho v \delta}{\pi} \end{aligned} \quad (3)$$

The signaling cost per time unit using Mobile IP is:

$$\begin{aligned} C_{mip} &= (6\alpha H_{mh-bs} + 6H_{bs-dhcp} + 2H_{dhcp-ha})\delta r_c \\ &= (6\alpha H_{mh-bs} + 6H_{bs-dhcp} + 2H_{dhcp-ha})\frac{\rho v \delta}{\pi} \end{aligned} \quad (4)$$

From Equation (3) and (4), we can observe that NGIneUS has an extra signaling cost due to shadow migration only inside the wired network, while reducing the wireless transmission costs. This is due to the user shadows handling the location update messages inside the wired network. In addition, with the same shadow migration overhead, the proposed scheme has less signaling cost than Mobile IP as α increases. In this condition, faster moving MHs or smaller subnet sizes make the performance of the proposed scheme superior to that of Mobile IP.

4. Conclusions

In this paper, we outlined the mobility management scheme of NGIneUS, for seamless roaming in 4G wireless overlay networks. A new mobile software entity called *user shadow* has been introduced to the wired networks, addressing the roaming needs of the mobile user. With the help of user shadows, most signaling interaction between mobile devices and wired networks is constrained to the wired links, reducing the dependence on the limited wireless bandwidth. Additionally, the novel concept of software IP mobility was introduced, enabling the mobile software entities (i.e., user shadows) to communicate using their own IP stack. Software IP mobility enhances the current IP mobility approaches and can help in providing with seamless mobility. The signaling cost analysis has shown that the proposed mobility management scheme consumes less wireless bandwidth than Mobile IP. The signaling cost depends on the migration overhead of the user shadows, requiring these to be as compact as possible.

Currently, we are in the process of implementing a software IP mobility testbed, to support IP communication and mobility of software entities as the first step towards our NGIneUS framework. We are in the process of designing and evaluating of protocols and algorithms for handoff management among heterogeneous systems. The

handoff decisions, made by user shadows, will be based not only on the technical considerations such as signal to noise ratio (SNR) but also on the information collected on the user's past behavior, i.e., on user profiles. Since user shadows represent the mobile users in the networks, the security problem like the authentication, authorization and accounting (AAA) association between users, user shadows and NGSs is also an important issue under investigation.

References

- [1] Y. Raivio, "4G – Hype or Reality," *Proceedings of the IEEE 3G Mobile Communication Technologies*, March, 2001.
- [2] U. Varshney, and R. Jain, "Issues in Emerging 4G Wireless Networks," *IEEE Computer Magazine*, pp. 94-96, June, 2001.
- [3] G.V. Záruba, W. Wu, M. J. Kumar, and S. K. Das, "NGIneUS: Intelligent User Shadows for Next Generation Wireless Services," *Technical Report*, The University of Texas at Arlington, 2002.
- [4] C. Perkins, Ed., "IP Mobility Support for IPv4," *IETF RFC 3344*, Aug. 2002.
- [5] A. Campbell, J. Gomez, C-Y. Wan, S. Kim, Z. Turányi, and A. Valkó, "Cellular IP," *IETF Draft*, draft-ietf-mobileip-cellularip-00.txt, January 2000, Work in Progress.
- [6] R. Ramjee, T. La Porta, S. Thuel, and K. Varadhan, "IP Micro-Mobility Support Using HAWAII," *IETF Draft*, draft-ramjee-micro-mobility-hawaii-01.txt, July 2000, Work in Progress.
- [7] A. Misra, S. Das, A. McAuley, A. Dutta, and S.K. Das, "IDMP: An Intra-Domain Mobility Management Protocol using Mobility Agents," *IETF Draft*, draft-mobileip-misra-idmp-00.txt, July 2000, Work in Progress.
- [8] T. Brown, and S. Mohan, "Mobility Management for Personal Communications Systems," *IEEE Transactions on Vehicular Technology*, vol. 46, pp. 269-278, May 1997.